UNITED STATES PATENT AND TRADEMARK OFFICE

W

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/834,334	04/12/2001	Bruce V. Hartley	005029.P018C	2402

30955 7590 05/18/2004

LATHROP & GAGE LC
4845 PEARL EAST CIRCLE
SUITE 300
BOULDER, CO 80301

EXAMINER
MILLER, CRAIG S

ART UNIT	PAPER NUMBER
2857	

DATE MAILED: 05/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/834,334	**Applicant(s)** HARTLEY ET AL.	
	Examiner Craig Miller	**Art Unit** 2857	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 04 March 2004.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-20 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

1. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

2. Claims 1-20 are rejected under 35 U.S.C. 103 as being unpatentable over CyberCop Scanner by Network Associates as described in Info World article entitled "**Test Center Comparison**" (hereafter referred to as 'CyberCop') in view of InfoWorld article entitled, "**The Ins and Outs of a Network Security Audit**" (hereafter referred to as 'Security Audit').

As to claims 1, 4, 11, 12, 14, 15 CyberCop discloses the instant invention essentially as claimed with the exception that CyberCop does not specify generating a configuration baseline or a file system database for use in other utility functions. CyberCop discloses a security system having a module analyzing portions of a network for identifying network vulnerabilities (page 2, forth paragraph from last) and a memory containing security information for performing the analysis (page 3, second from last paragraph), but is not specifically disclosed as providing suggested fixes though the article implies such (see page 2, second from last paragraph). Because it is well known to repair known security flaws and because it is known to automate that which was known to done manually, In re Venner, 120 USPQ 192 (CCPA 1958), "*Furthermore, it is well settled that it is not 'invention' to broadly provide a mechanical or automatic means to replace manual activity which has accomplished the same result.*", it would have been obvious to one of ordinary skill in the art at the time the invention was made to include within the device of CyberCop an automated security flaw repair module so as to receive the obvious benefit derived therefrom such as repairing known network security flaws. As to generating a configuration baseline or a file system database for use in other utility functions, Security Audit discloses on page 4, first paragraph that network audit results should be stored for comparison to future audits (system configuration and vulnerability baseline determined by the audit). Because CyberCop and the teachings of Security Audit are within the art of network security, because Security Audit teaching maintaining reports for comparison to future audits and because such computerized reports are commonly stored in the form of a database, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include within the device of CyberCop the storing of a baseline audit configuration within a database for future reference so as to receive the expected benefits derived there from such as enhanced system flexibility and determination of network configuration and vulnerability histories absent a showing of unexpected results or synergistic effects from any particular claimed combination.

As to claims 2, 3, 8 and 19, CyberCop uses a graphical user interface (see screen snapshot from SoftSeek.com).

As to claims 5 and 13, said claims are directed towards a utility module capable of repairing detected security flaws. CyberCop does not specifically disclose automating the fixes suggested. Because it is well known to repair known security flaws, because it is well known that supervisory utilities are used to fix security flaws and because it is known to automate that which was known to done manually, In re Venner, 120 USPQ 192 (CCPA 1958), "*Furthermore, it is well settled that it is not 'invention' to broadly provide a mechanical or automatic means to replace manual activity which has accomplished the same result.*", it would have been obvious to one of ordinary skill in the art at the time the invention was made to include within the device of CyberCop an automated security flaw repair module, including a supervisory module, so as to receive the obvious benefit derived therefrom such as repairing known network security flaws absent a showing of unexpected results or synergistic effects from any particular claimed combination.

As to claims 6, 7 and 20, CyberCop supports Unix network environments (see page 10 bottom).

As to claims 9 and 16, CyberCop discloses an upgradable list of vulnerabilities (see bottom of page 4).

As to claims 10 and 18, CyberCop is disclosed as supporting password cracking (page 3 second from last paragraph) but does not specify using a dictionary. Because it is known in general to use dictionaries to break password files and because CyberCop discloses password cracking, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include within the system of CyberCop a dictionary so as to use a well known method to break password files so as to receive the obvious benefits derived therefrom such as enhanced system security absent a showing of unexpected results or synergistic effects from any particular claimed combination.

As to claim 17, said claim includes detecting if excessive system services are running. Because the theft of processing time is one of the most common byproducts of intrusions into a network, because the overwriting of logs to cover-up such theft is well known, because monitoring CPU usage real-time is extremely well known, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include within the system of CyberCop a CPU usage monitor so as to receive the obvious benefits derived therefrom such as enhanced system security absent a showing of unexpected results or synergistic effects from any particular claimed combination.

3. Applicant's arguments filed 4 March 2004 have been fully considered but they are not persuasive.

While the review article describing CyberCop was indeed published after filing of Applicant's provisional application, the product existed for public use as of 27 February 1998 as evidenced by Network Associates press released of 17 February 1998 and already of record in the instant application (see bottom of page 1), "*The CyberCop system ships on February 27, 1998...*" Therefore, because the rejections are based upon the CyberCop software (as described in the review article, CyberCop) and because the CyberCop software predates Applicant's priority, the rejection is deemed proper and is hereby retained.

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

5. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Craig Steven Miller whose telephone number is (571) 272-2219. Art Unit facsimile services are now available at (703) 872-9306.

The Examiner can normally be reached on Mondays, Tuesdays and Thursdays from 07:30am - 4:00pm EDT. Should repeated attempts to reach the Examiner be unsuccessful, the Examiner's Supervisor, Marc Hoff may be reached at (571) 272-2216.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2800.

Craig Steven Miller (ss)
11 May 2004

HAL WACHSMAN
PRIMARY EXAMINER
AU2857